BM CYBER SECURITY
locally focused, globally aware

BOB MANN
DIRECTOR
Phone: +44 (0)7977 460393
Email: bob.mann@bmcybersecurity.com
Website: www.bmcybersecurity.com

Tales from the trenches

FROM A CHIEF INFORMATION SECURITY OFFICER (CISO)

Plus ça change, plus c'est la même chose…

The more things change, the more they stay the same…

Čím více se věci mění, tím více zůstávají stejné…

Who am I to stand here…it all began nearly 40 years ago…

Like many before me I was young, fit, slim, enthusiastic, handsome(?), who wanted to conquer the planet: go everywhere, see everything, discover all…

…so where did it all go wrong?

Introduction

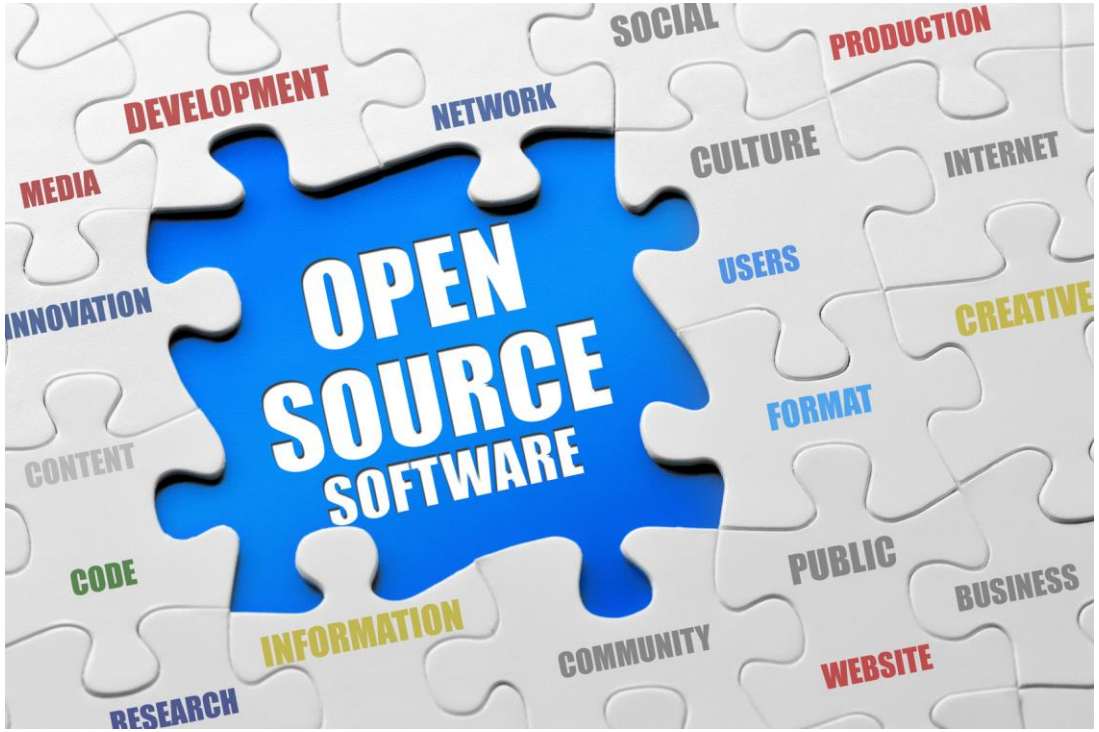
Cyber security - why I remain nervous…

- Many things are outside my control
- Is open source software safe – sometimes!
- Lack of realisation that a real threat exists
- Developers and everyone else operate at different speeds
- Sales & Marketing teams often act like hooligans because IT cannot move fast enough
- Increase in threat actors and their capabilities
- Technology moves at a blistering pace
- Malware (viruses) going since 1971…

Direction isn't always straightforward…

Open source code - good

- The quality of open source code is improving
- Code review software (both static and dynamic) is now very reliable and providing comfort to CISOs'
  - Black Duck report, open source components are now present in 96 percent of commercial applications
- Fear for security officers is that there's a lack of control, of transparency. Coders go 'off piste' all the time. However:
  - Permits quicker repairs
  - Allegedly higher-quality Apps



Specialist skills…

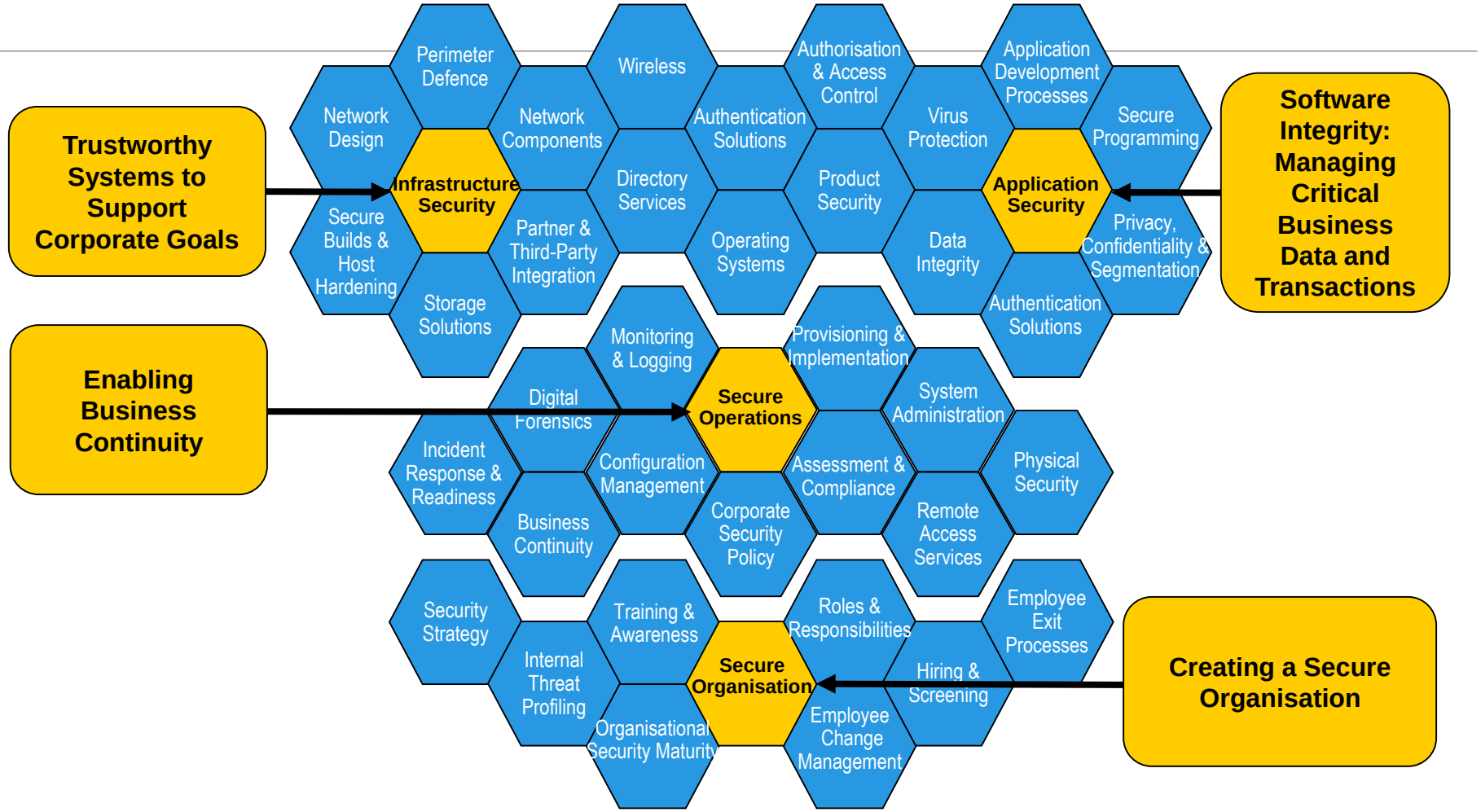
Open source code - bad

- The average application had 147 different open source components -- and 67 percent of the applications used components with known vulnerabilities
- Veracode report, only 28 percent of organisations do any kind of regular analysis to find out what components are built into their applications
- DevOps move at a pace that everyone else finds difficulty in keeping up
- Distrust of ‘non-verifiable’ codebase

Ever increasing gaps…

Security – a business discipline

When protecting business data and services Information Security has a wide and diverse coverage



Threats

OFFENCE & DEFENCE

‘Extreme’ unauthorised access - PLA Unit 61398

- Been in operation for at least 6 years that we know of…
- Mandiant report of 2016 gives additional details
- Forensic evidence traces the base of operations to a 12-story building off Datong Road in a public, mixed-use, area of Pudong, Shanghai, China
- Huge complex housing more than 1,000 computer servers and an army of linguists, researchers and other technicians working in support of the hackers
- In 2015,Barak Obama and Chinese President Xi Jinping agreed *not* to engage in espionage against each other!
- Intrusion periods to detection vary from 150 to 335 days
- The global median time from compromise to discovery has dropped significantly from 146 days in 2015 to 99 days in 2016
- Forensic examiners: some intrusions were 5+ years old

Budget: $147 Billion

IMVHO – supporting threat challenges

Flat networks are a real pain: no bulkheads fitted to hinder or obstruct intruders, or restrict damage

Privileged access: local Admin credentials are often poorly managed

Inadequate security by default and design

Silo'd mentality between internal teams

InfoSec teams often viewed as "superior" – poor understanding and communication

Lack of independent health checks

Noticeable lack of preparedness AND response

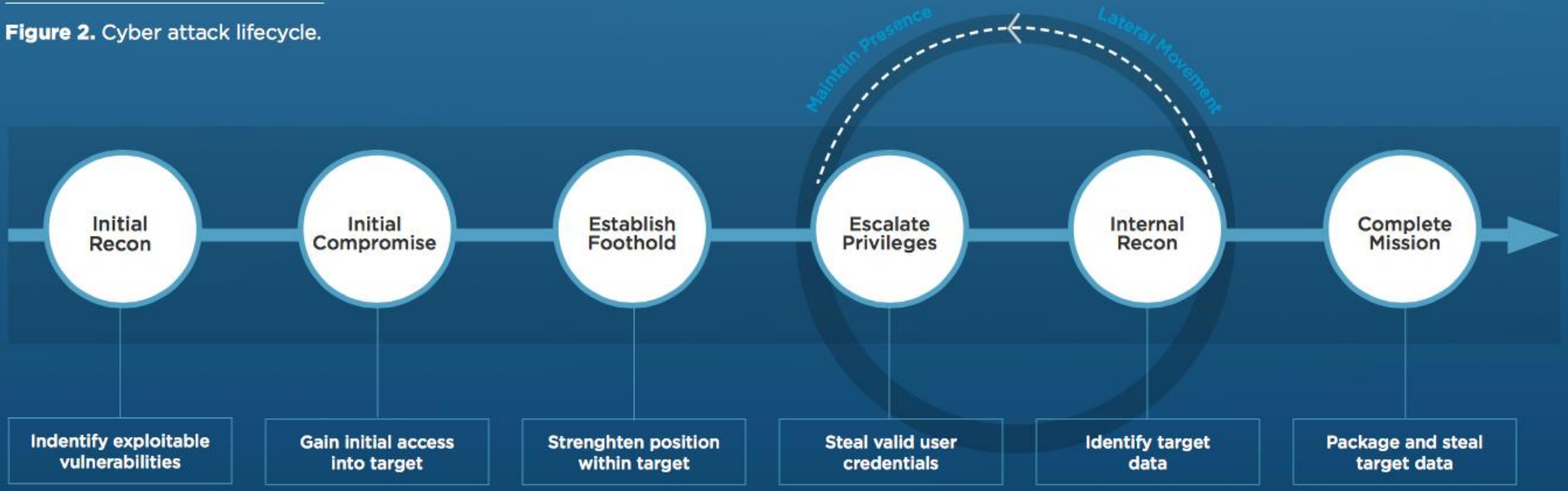
Case studies

OFFENCE & DEFENCE

Case study I – Tiger Team Test - approach

The following section details the more significant changes we have witnessed while investigating financial attackers. The changes are grouped in accordance with the attack lifecycle diagram.

Figure 2. Cyber attack lifecycle.



Mandiant M-Trends 2017 report

Case study I – Tiger Team Test

Also known as Red Team Testing

InfoSec team sceptical of the veracity of IT status information:

- A “gloves off” covert intrusion: covering physical and electronic targets
- Only 4 people knew that the test was taking place
- Selected targets by the attack team

Network “owned” in just a few hours 😱

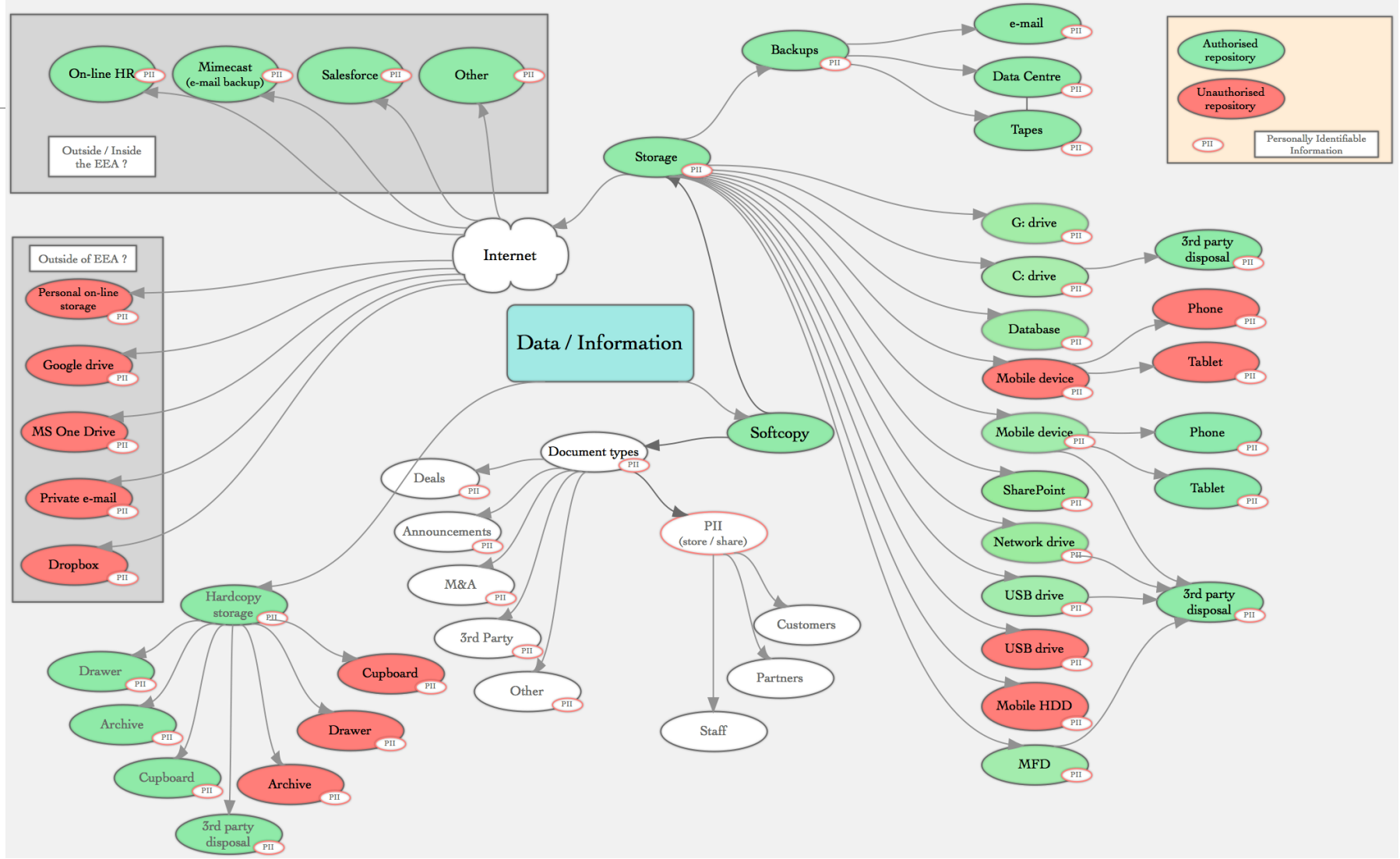
Exec Board were given a personal brief:

- This was a game changer…

Case study II – data repository cursory check

Another case study: As advised it would be a smart move to fully understand how your organisation handles it structured and unstructured data.

Don't be surprised at what you uncover: start with the mind-set that you will fix things you discover…



Case study III – data theft

Temporary staff member

Using an iPhone

Taking photographs of financial document belonging to customers

Unfortunately *R (*dep't name obfuscated!*) escorted culprit from premises before seeking specialist help

Legal discussions and ICO notified

InfoSec provided counter-compromise direction

12 months Experian checks for potential victims

Civilian police force involved – far too late

Outcome: evidence lost – no prosecution 😭

Counter-measures

OFFENCE & DEFENCE

Temperature control…

Common sense!!!

- Somehow, in the fog of information technology people lose their sense of perspective
- Because things aren't in their faces they often forget that there are any threats out their in the wild

Pulled in too many directions…

Possible to stop attacks?

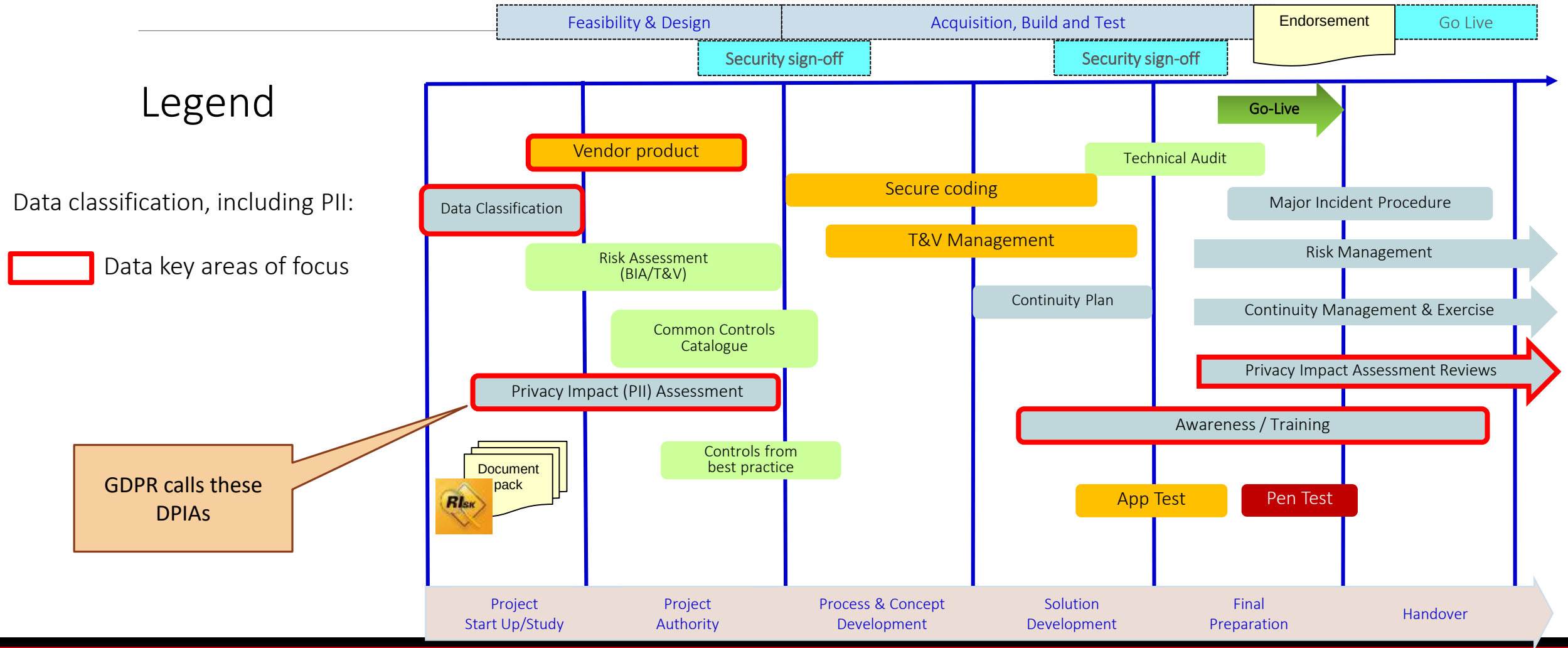
No. We need to get real about our inability – and stop mimicking an ostrich…

Top 10 breach vectors:

1. Carelessness
2. Users in a rush
3. Lack of respect for data value
4. Poor incident response
5. Taken for granted
6. Sensitive data / PII on endpoints
7. Attackers more technically advanced than us
8. Cyber threat actors have absolutely no rules
9. Many are fully sponsored
10. It's an IT problem

* Source: Cisco & Trend Micro

Security in the Project Lifecycle



Countermeasures

What does the term *appropriate level* of security really mean?

KISS principle – it works every time

If you can't monitor you can't manage

If you can't manage you can't report

If you can't report you can't analyse

If you can't analyse correctly you can't respond effectively

Deploy only hardened systems

Maintain (re-configure, patch and update quickly)

CMDB currency poor, lack (or accuracy) of an asset list is testimony of the effort being expended

Credible data management, data governance

Summary

Takeaways

- Whether writing applications or tools be mindful that there are so many users depending on your expertise
- Right first time: secure by design
- Consider just how good software is at protecting your personal data
- Like Cyber security, open source is also gaining a foothold
- Don’t forget to have fun!

TAKEAWAY II

There’s an old Chinese proverb:

"If you want 1 year of prosperity, grow grain. If you want 10 years of prosperity, grow trees. If you want 100 years of prosperity, grow people”

We say:

“Turning frogs into princes by kissing them rarely works!”

Děkuji, bylo to potěšení

When I first introduced myself, I mentioned that many years ago I was extremely fit and often undertook assignments to probe security defences.

I thought it might be good way to bow out and relate the story of the largest object I was asked to ‘borrow’

Gives you quite a large edge…

Questions: anglicky prosím ☺

Děkuji, bylo mi potěšením